ICS 03.100.01
A 02

中华人民共和国国家标准

GB/T 26318—2010

物流网络信息系统风险与防范

Logistics network information systems risk and prevention

2011-01-14 发布　　2011-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中华人民共和国商务部提出并归口。

本标准起草单位：浙江双马国际货运有限公司、深圳市联合纵横国际货运代理有限公司、新景程国际物流有限公司、中国国际电子商务有限公司、全国国际货运代理标准化技术委员会、中外运长航集团有限公司、中国海运（集团）总公司、中国中钢集团公司、锦程物流（集团）公司、北京交通大学、中钢国际货运有限公司、上海宝霖国际危险品物流有限公司、福建金航国际货运代理有限公司厦门分公司、上海港虹信息科技有限公司、厦门通程物流有限公司、内蒙古安快物流集团、新时代保险经纪有限公司、新疆德鲁亚国际物流有限公司、新疆托木尔货运代理有限责任公司。

本标准主要起草人：林忠、王喜富、蒋寒松、胡荣、杨爽、陈峥、冯建萍、杨旭、景洪德、张海峰、陈智勇、李莉丽。

引　言

本标准通过对物流信息资产、面临的威胁、资产存在的脆弱性以及脆弱性被威胁利用后所产生的实际负面影响等进行识别、分析，从而得到资产、威胁和脆弱性相映射的资产价值、威胁等级和薄弱点等级等，转化成以提示的形式给出了物流基础数据风险、实体风险、硬件风险、软件风险和管理风险五个方面的主要风险来源和相应的防范措施，以对付威胁、减少脆弱性、限制意外事件影响，实现以下一种或多种功能：预防、延迟、阻止、检测、限制、修正、恢复、监控以及意识性提示或强化。

当前，由于我国中、小物流企业占多数，而企业规模、服务水平、人员素质、地域等差异不一，导致企业在信息化建设和技术运用与其实际的经营规模、业务范围、流程和管理之间发展不平衡，制约了企业和行业的信息化的发展，加大了企业的运营风险。本标准旨在提高中、小物流企业的物流网络信息风险防范的能力。

物流网络信息系统风险与防范

1 范围

本标准规定了物流网络信息系统的风险评估、安全防范措施和安全管理要求。

本标准适用于我国物流企业对信息系统或物流信息系统公共服务平台进行规范与管理，并可作为相关机构对物流网络信息系统进行安全评价的依据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

资产 asset

对组织具有价值的信息或资源，是安全策略保护的对象。

[GB/T 20984—2007，定义 3.1]

3.2

资产价值 asset value

资产的重要程度或敏感程度的表征。资产价值是资产的属性，也是进行资产识别的主要内容。

[GB/T 20984—2007，定义 3.2]

3.3

威胁 threat

可能导致对系统或组织危害的不希望事故潜在起因。

[GB/T 20984—2007，定义 3.17]

3.4

薄弱点 vulnerability

资产或资产组中能被威胁利用的弱点。

3.5

风险 risk

特定的威胁利用资产的一种或一组薄弱点，导致资产的损害的潜在的可能性，即特定威胁事件发生的可能性与后果的结合。

3.6

信息系统的风险 information system risk

特定的威胁利用信息资产的漏洞或弱点从而造成对资产的一种潜在损害，包括信息资产、威胁和自身的漏洞或弱点三个组成部分。

注：信息系统风险的严重程度可用资产受损害的程度与威胁发生的概率的乘积来衡量。